

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-110210

(43)Date of publication of application : 23.04.1999

(51)Int.Cl.
G06F 9/06
G06F 9/06
G06F 12/14

(21)Application number : 09-268815 (71)Applicant : NEC CORP

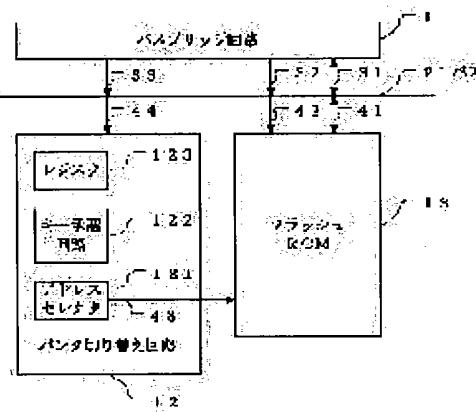
(22)Date of filing : 01.10.1997 (72)Inventor : NISHIKAWA SATOSHI

(54) EXPANDED BIOS PROTECTION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a basic input output operating system(BIOS) protection system that secures a security for an access from a user.

SOLUTION: An authentication key for admitting an access of an expanded BIOS is set in advance in a key approval circuit 122 of a bank changeover circuit, and in the BIOS expansion access, a user inputs the authentication key. The inputted identification key is compared with an authentication key inside of the key approval circuit 122. An address which accesses the expanded BIOS is set in an address register 123 and when the comparison result coincides, an address selector 121 outputs an address for accessing the expanded BIOS to an address line 43 and the expanded BIOS of a subordinate bank of a flash ROM 13 becomes accessible.



LEGAL STATUS

[Date of request for examination] 01.10.1997

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3039479

[Date of registration] 03.03.2000

[Number of appeal against examiner's
decision of rejection]

[Date of requesting appeal against
examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平11-110210

(43)公開日 平成11年(1999)4月23日

(51)Int.Cl.⁶

G 06 F 9/06

12/14

識別記号

5 5 0

5 4 0

3 1 0

F I

G 06 F 9/06

12/14

5 5 0 J

5 4 0 L

3 1 0 A

審査請求 有 請求項の数 6 OL (全 6 頁)

(21)出願番号

特願平9-268815

(22)出願日

平成9年(1997)10月1日

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 西川 聰

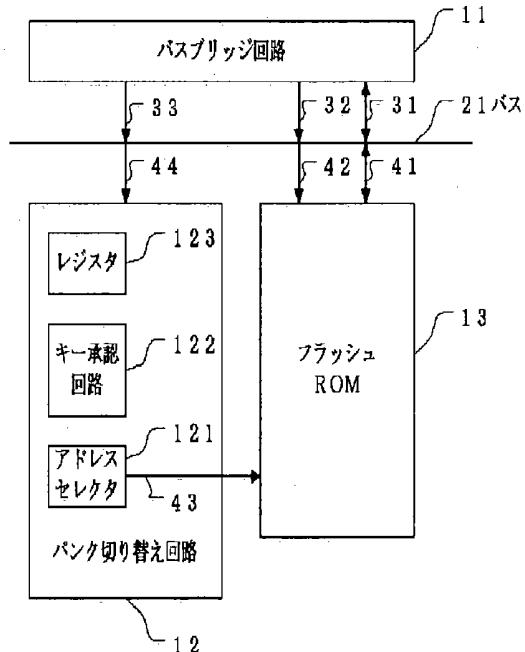
東京都港区芝五丁目7番1号 日本電気株
式会社内

(74)代理人 弁理士 京本 直樹 (外2名)

(54)【発明の名称】 拡張B IOS保護システム

(57)【要約】

【課題】 ユーザーからのアクセスに対しセキュリティを確保した拡張B IOS保護システムを実現する。
【解決手段】 バンク切り替え回路12のキー承認回路122には、あらかじめ拡張B IOSのアクセスを許可する認証キーが設定され、拡張B IOSアクセス時には、ユーザーが認証キーを入力する。入力された認証キーは、キー承認回路122内の認証キーと比較される。アドレスレジスタ123に拡張B IOSをアクセスするアドレスを設定し、かつ比較結果が一致すると、アドレスセレクタ121は拡張B ISOをアクセスするアドレスをアドレス線43に出力し、フラッシュROM13の下位バンクの拡張B IOSがアクセス可能となる。



【特許請求の範囲】

【請求項1】(a) 上位バンクに標準B IOSを格納し、下位バンクに拡張B IOSを格納するフラッシュROMと、(b) 前記標準B IOSをアクセスするのか前記拡張B IOSをアクセスするのかを指定する情報を格納するレジスタと、前記拡張B IOSのアクセスを許可する第1の認証キーを保持し前記拡張B IOSのアクセス時に操作者により入力された第2の認証キーと前記第1の認証キーとを比較し比較結果を出力するキー承認回路と、前記レジスタの出力が前記拡張B IOSを示しかつ前記キー承認回路の出力が比較一致を示した場合に前記下位バンクの拡張B IOSを指示するアドレスを出力するアドレスセレクタとを備えるバンク切り替え回路と、を有することを特徴とする拡張B IOS保護システム。

【請求項2】前記第1の認証キーを格納する認証キー レジスタと、前記第2の認証キーを格納する入力レジスタと、前記認証キーレジスタの出力および前記入力レジスタの出力を比較する比較回路と、前記比較回路の出力を格納し、前記アドレスセレクタに出力する前記キー承認回路を有することを特徴とする請求項1記載の拡張B IOS保護システム。

【請求項3】CPUと、バスブリッジ回路と、前記CPUおよび前記バスブリッジ回路を接続する第1のバスと、前記バンク切り替え回路と、前記フラッシュROMと、前記バスブリッジ回路および前記バンク切り替え回路、前記バスブリッジ回路および前記フラッシュROMを接続する第2のバスとを有することを特徴とする請求項1または2記載の拡張B IOS保護システム。

【請求項4】(a) 複数バンクのそれぞれに各種B IOSを含むプログラムを格納するN(N>2)バンク構成のフラッシュROMと、(b) 前記複数バンクのうちどのバンクをアクセスするのかを指定する情報を格納するレジスタと、前記各バンクのアクセスを許可するN個の第1の認証キーを保持し前記拡張B IOSのアクセス時に操作者により入力された第2の認証キーと前記第1の認証キーとを比較し比較結果を出力するキー承認回路と、前記レジスタの出力が前記各バンクを示しかつ前記キー承認回路の出力が比較一致を示した場合に前記バンクを指示するアドレスを出力するアドレスセレクタとを備えるバンク切り替え回路と、を有することを特徴とする拡張B IOS保護システム。

【請求項5】前記N個の第1の認証キーを格納する認証キーレジスタと、前記第2の認証キーを格納する入力レジスタと、前記認証キーレジスタの出力および前記入力レジスタの出力を比較する比較回路と、前記比較回路の出力を格納し、前記アドレスセレクタに出力する前記キー承認回路を有することを特徴とする請求項4記載の拡張B IOS保護システム。

【請求項6】CPUと、バスブリッジ回路と、前記C

P Uおよび前記バスブリッジ回路を接続する第1のバスと、前記バンク切り替え回路と、前記フラッシュROMと、前記バスブリッジ回路および前記バンク切り替え回路、前記バスブリッジ回路および前記フラッシュROMを接続する第2のバスとを有することを特徴とする請求項4または5記載の拡張B IOS保護システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、拡張B IOS保護システムに関し、特に、認証キーによりB IOSの内容を保護する拡張B IOS保護システムに関する。

【0002】

【従来の技術】従来、コンピュータにおいて、ベーシック・インプット・アウトプット・オペレーティング・システム(以降、B IOSと記す)は、フラッシュROM等で構成され、再書き込みが可能となっている。

【0003】また、機能の多様化に伴い、基本的な機能が含まれる標準B IOSと付加的な機能が含まれる拡張B IOSとの2種類のB IOSを持つコンピュータが増加している。

【0004】この種の技術としては、たとえば、「特開平8-69376号公報」記載の技術が存在する。

【0005】この公報記載の「B IOSの書き換え制御回路」は、B IOSを格納する不揮発メモリを上位部分・下位部分に機能分割し、上位部分に標準B IOSを、下位部分に拡張B IOSを格納したものである。そして、B IOSの書き換えに際し、まず、下位部分に新しい基本B IOSを書き込み、基本B IOSが常に存在するようにし、B IOSの書き込みの途中に予期せぬ電源断が発生しても、コンピュータの動作が回復できるようしている。

【0006】

【発明が解決しようとする課題】上述した従来の技術の問題点は、不揮発ROM、フラッシュROM等に格納されたB IOSに対するセキュリティーが確保できないことである。その理由は、不揮発ROMやフラッシュROM内に保存しているB IOSは、起動中からOS起動後にいたるまで、CPU等からのアクセス可能空間に存在するため、ユーザによって容易に読み出し、または書き込みすることができるからである。

【0007】本発明の目的は、ユーザーからのアクセスに対しセキュリティーを確保した拡張B IOS保護システムを実現することである。

【0008】

【課題を解決するための手段】本発明の第1の拡張B IOS保護システムは、(a) 上位バンクに標準B IOSを格納し、下位バンクに拡張B IOSを格納するフラッシュROMと、(b) 前記標準B IOSをアクセスするのか前記拡張B IOSをアクセスするのかを指定する情報を格納するレジスタと、前記拡張B IOSのアクセス

を許可する第1の認証キーを保持し前記拡張BIOSのアクセス時に操作者により入力された第2の認証キーと前記第1の認証キーとを比較し比較結果を出力するキー承認回路と、前記レジスタの出力が前記拡張BIOSを示しかつ前記キー承認回路の出力が比較一致を示した場合に前記下位バンクの拡張BIOSを指示するアドレスを出力するアドレスセレクタとを備えるバンク切り替え回路と、を有する。

【0009】本発明の第2の拡張BIOS保護システムは、前記第1の拡張BIOS保護システムであって、前記第1の認証キーを格納する認証キーレジスタと、前記第2の認証キーを格納する入力レジスタと、前記認証キーレジスタの出力および前記入力レジスタの出力を比較する比較回路と、前記比較回路の出力を格納し、前記アドレスセレクタに出力する前記キー承認回路を有する。

【0010】本発明の第3の拡張BIOS保護システムは、前記第1または第2の拡張BIOS保護システムであって、CPUと、バスブリッジ回路と、前記CPUおよび前記バスブリッジ回路を接続する第1のバスと、前記バンク切り替え回路と、前記フラッシュROMと、前記バスブリッジ回路および前記バンク切り替え回路、前記バスブリッジ回路および前記フラッシュROMを接続する第2のバスとを有する。

【0011】本発明の第4の拡張BIOS保護システムは、(a)複数バンクのそれぞれに各種BIOSを含むプログラムを格納するN(N>2)バンク構成のフラッシュROMと、(b)前記複数バンクのうちどのバンクをアクセスするのかを指定する情報を格納するレジスタと、前記各バンクのアクセスを許可するN個の第1の認証キーを保持し前記拡張BIOSのアクセス時に操作者により入力された第2の認証キーと前記第1の認証キーとを比較し比較結果を出力するキー承認回路と、前記レジスタの出力が前記各バンクを示しかつ前記キー承認回路の出力が比較一致を示した場合に前記バンクを指示するアドレスを出力するアドレスセレクタとを備えるバンク切り替え回路と、を有する。

【0012】本発明の第5の拡張BIOS保護システムは、前記第4の拡張BIOS保護システムであって、前記N個の第1の認証キーを格納する認証キーレジスタと、前記第2の認証キーを格納する入力レジスタと、前記認証キーレジスタの出力および前記入力レジスタの出力を比較する比較回路と、前記比較回路の出力を格納し、前記アドレスセレクタに出力する前記キー承認回路を有する。

【0013】本発明の第6の拡張BIOS保護システムは、前記第4または第5の拡張BIOS保護システムであって、CPUと、バスブリッジ回路と、前記CPUおよび前記バスブリッジ回路を接続する第1のバスと、前記バンク切り替え回路と、前記フラッシュROMと、前記バスブリッジ回路および前記バンク切り替え回路、前

記バスブリッジ回路および前記フラッシュROMを接続する第2のバスとを有する。

【0014】

【発明の実施の形態】次に、本発明の第1の実施の形態について図1～図5を参照して詳細に説明する。図1は、本発明の第1の実施の形態を示すブロック図である。図1を参照すると、本発明の第1の実施の形態は、CPU10と、バスブリッジ回路11と、バンク切り替え回路12と、フラッシュROM13と、NVRAM14と、CPU10およびバスブリッジ回路11が接続されるバス20と、バスブリッジ回路11、バンク切り替え回路12、およびNVRAM14が接続されるバス21とから構成される。

【0015】図2は、フラッシュROM13の構成を示すブロック図である。図2を参照すると、フラッシュROM13は、標準BIOSが格納される上位バンク131と、拡張BIOSが格納される下位バンク132との2バンク構成をとる。アドレス80000～40001h(16進)で指定される上位バンク131に標準BIOSが格納され、アドレス40000～00000h(16進)で指定される下位バンク132に拡張BIOSが格納される。

【0016】図3は、図1の一部(バスブリッジ回路11、バンク切り替え回路12、およびフラッシュROM13)の詳細を示すブロック図である。図3を参照すると、バスブリッジ回路11は、バス21と、データ線31およびアドレス線32により接続される。また、バスブリッジ回路11は、バス21と制御線33により接続される。バンク切り替え回路12は、バス21と制御線44により接続され、また、フラッシュROM13とアドレス線43により接続される。フラッシュROM13は、バス21とデータ線41およびアドレス線42により接続される。アドレス線43の状態が「オン」であれば、上位バンクの標準BIOSがアクセスされ、「オフ」であれば、下位バンク132の拡張BIOSがアクセスされる。

【0017】バス21において、データ線31、アドレス線32、制御線33は、それぞれデータ線41、アドレス線42、制御線44と接続される。また、バンク切り替え回路12は、アドレスセレクタ121、キー承認回路122、およびレジスタ123を備えている。

【0018】図4は、アドレスセレクタ121の詳細を示すブロック図である。図4を参照すると、アドレスセレクタ121は、キー承認回路122の出力とレジスタ123の出力との論理和を出力する論理回路で構成される。

【0019】図5は、キー承認回路122の詳細を示すブロック図である。図5を参照すると、キー承認回路122は、認証キーレジスタ1221と比較回路1222と出力レジスタ1223と入力レジスタ1224とを備

えている。

【0020】次に、本発明の第1の実施の形態の動作について図6を参照して説明する。図6は、本発明の第1の実施の形態を示すフローチャートである。あらかじめ、以下の処理が行われる。ユーザーにより、NVRAM14に、拡張BIOSに対するアクセスを許可するかどうかを示す許可情報が書き込まれる。この処理は、ユーザーからの指示により、CPU10、バス20、バスブリッジ回路11、NVRAM14の経路で行われる。また、キー承認回路122内の認証キーレジスタ1221に拡張BIOSに対するアクセスを許可する認証キーが書き込まれる。この処理は、ユーザーからの指示により、ユーザーからの指示により、CPU10、バス20、バスブリッジ回路11、制御線33、バス21、制御線44、キー承認回路122の経路で行われる。

【0021】次に、初期状態について説明する。初期状態において、レジスタ123、出力レジスタ1223は、ともに「オン」に設定される、アドレスセレクタ121の出力は「オン」となり、さらに、アドレス線43が「オン」となる。したがって、初期状態では、フラッシュROM13は上位バンク131の標準BIOSがアクセスされる。

【0022】電源が「オン」になると（図6A1）、標準BIOS内の自己診断プログラムが主記憶（図示しない）にロードされ実行が開始され、診断が実行される（図6A2）。次に、NVRAM14内の許可情報を参照し、拡張BIOSに対するアクセスが許可されているかどうか確認する（図6A3）。アクセスが許可されていなければ、拡張BIOSへのアクセスは実施せず、診断を終了する。拡張BIOSへのアクセスが許可されていると、自己診断プログラムは、ディスプレイ（図示せず）に拡張BIOSアクセスのための認証キーを入力することを要求するメッセージを表示する（図6A4）。ユーザーは、このメッセージに対する応答として、キーボード（図示せず）から認証キーを入力する。自己診断プログラムは、入力された認証キーをCPU10、バス20、バスブリッジ回路11、制御線33、バス21、制御線44の経路でバンク切り替え回路12のキー承認回路122へ送出する（図6A5）。

【0023】キー承認回路122では、入力された認証キーが入力レジスタ1224に保持され、認証キーレジスタ1221内の認証キーと比較回路1222により比較され（図6A6）、結果が一致しないと、出力レジスタ1223が「オン」に設定され、結果が一致すると出力レジスタ1223が「オフ」に設定される。出力レジスタ1223が「オフ」に設定されると、キー承認回路122の出力が「オフ」になる。

【0024】次に、自己診断プログラムにより、CPU10、バス20、バスブリッジ回路11、制御線33、バス21、制御線44の経路でバンク切り替え回路12

のレジスタ123が「オフ」に設定される（図6A7）。

【0025】キー承認回路122の出力、レジスタ123が共に「オフ」になると、アドレスセレクタ121の論理回路の出力は「オフ」になり、アドレス線43は「オフ」になり、したがって、フラッシュROM13の下位バンク132の拡張BIOSがアクセス可能となる（図6A8）。

【0026】次に、自己診断プログラムにより、フラッシュROM13の下位バンク132から拡張BIOSが主記憶（図示せず）にロードされる（図6A9）。すなわち、CPU10、バス20、バスブリッジ回路11、アドレス線32、バス21、アドレス線42の経路でフラッシュROM13にアドレスが与えられ、同時に、バンク切り替え回路12からアドレス線43のアドレスが与えられ、データ線41、バス21、データ線31、バスブリッジ回路11、バス20、の経路で拡張BIOSがCPU10に読み出され、さらに、主記憶（図示せず）にロードされる。

【0027】バス21拡張BIOSのロードが終了すると、自己診断プログラムによりレジスタ123が「オン」に、出力レジスタ1223が「オン」に設定され、アドレス線43は「オン」となり、拡張BIOSへのアクセスの代わりに標準BIOSへのアクセスが可能となる（図6A10）。

【0028】次に、自己診断プログラムは、主記憶の拡張BIOSを実行する（図6A11）。

【0029】次に、本発明の第2の実施の形態について説明する。本発明の第2の実施の形態は、第1の実施の形態とフラッシュROM13のバンク数が異なる。バンク数は、2のN乗（ $N > 1$ ）であり、したがって、レジスタ123はNビット、アドレス線43もNビットである。この構成により、多種のBIOSを切り替えてアクセスすることが可能となる。また、認証キーも各バンクに対応して設定可能である。

【0030】また、以上は、BIOSに関して説明したが、フラッシュROM13には、種々のプログラム、データ等を格納することが可能である。

【0031】

【発明の効果】本発明の効果は、フラッシュROM内の拡張BIOSに対してセキュリティを確保することができるようである。その理由は、拡張BIOSは通常アクセス不可の領域に格納されており、さらに、認証キーを知っているユーザーによってのみアクセス可能とすることができるからである。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態を示すブロック図である。

【図2】図1のフラッシュROMの構成を示すブロック図である。

【図3】図1の一部の詳細を示すブロック図である。

【図4】図1のアドレスセレクタの詳細を示すブロック図である。

【図5】図1のキー承認回路の詳細を示すブロック図である。

【図6】本発明の第1の実施の形態の動作を示すフローチャートである。

【符号の説明】

1 0	CPU
1 1	バスブリッジ回路
1 2	バンク切り替え回路
1 3	フラッシュROM
1 4	NVRAM
2 0	バス

2 1 バス

3 1 データ線

3 2 アドレス線

3 3 制御線

4 1 データ線

4 2 アドレス線

4 3 アドレス線

4 4 制御線

1 3 1 上位バンク

1 3 2 下位バンク

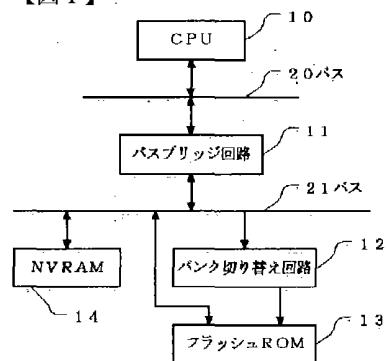
1 2 2 1 認証キーレジスタ

1 2 2 2 比較回路

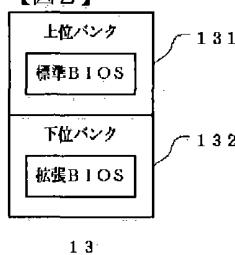
1 2 2 3 出力レジスタ

1 2 2 4 入力レジスタ

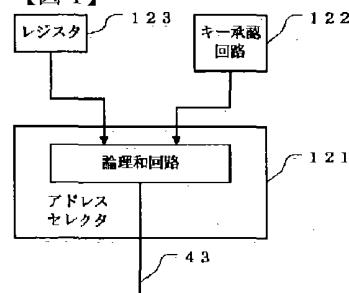
【図1】



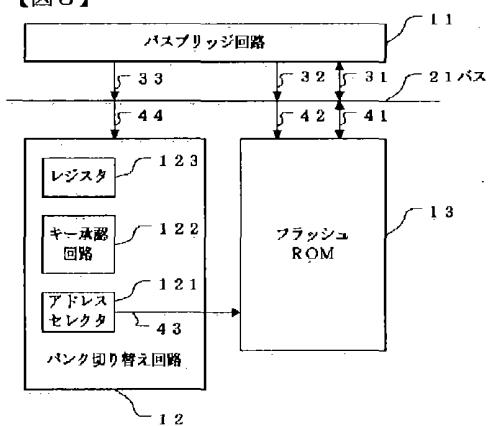
【図2】



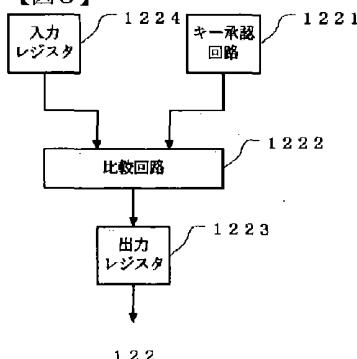
【図4】



【図3】



【図5】



【図6】

